IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

Claims 1-37 (Canceled).

38. (New) A personal security device (PSD) that generates a digital certificate, the PSD comprising:

a first encryption component that encrypts a unique device identifier for the PSD to produce an encrypted unique device identifier;

a second encryption component that encrypts first contextual attributes of the PSD to produce encrypted first contextual attributes;

a first combiner that combines the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes for generating the digital certificate, wherein

the unique device identifier and first contextual attributes are encrypted using different encryption keys.

39. (New) The PSD of claim 38, further comprising:

a third encryption component that encrypts the combined encrypted first contextual attributes, encrypted unique device identifier, and unique device identifier to produce an encrypted message authentication code (MAC); and

a second combiner that combines the encrypted MAC with the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes in the digital certificate.

40. (New) The PSD of claim 38, wherein:

the unique device identifier is encrypted with an asymmetric encryption key; and

the first contextual attributes are encrypted with a symmetric encryption key.

41. (New) The PSD of claim 39, wherein:

the unique device identifier is encrypted with an asymmetric encryption key;

the first contextual attributes are encrypted with a first symmetric encryption key; and

the MAC is encrypted with a second symmetric encryption key.

42. (New) The PSD of claim 38, wherein the first combiner combines second contextual attributes of the PSD with the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes for generating the digital certificate.

43. (New) The PSD of claim 42, further comprising:

a third encryption component that encrypts the combined encrypted first contextual attributes, second contextual attributes, encrypted unique device identifier, and unique device identifier to produce an encrypted message authentication code (MAC); and

a second combiner that combines the encrypted MAC with the unique device identifier, the encrypted unique device identifier, the encrypted first contextual attributes, and the second contextual attributes in the digital certificate.

44. (New) The PSD of claim 43, wherein:

the unique device identifier is encrypted with an asymmetric encryption key;

the first contextual attributes are encrypted with a first symmetric encryption key; and

the MAC is encrypted with a second symmetric encryption key.

45. (New) A host for validating a digital certificate that is received from a personal security device (PSD), the host comprising:

a first decryption component that decrypts an encrypted unique device identifier for the PSD, which is received in the digital certificate, to produce a decrypted unique device identifier;

a second decryption component that decrypts encrypted first contextual attributes of the PSD, which are received in the digital certificate, to produce decrypted first contextual attributes;

a first comparator that compares the decrypted unique device identifier to a unique device identifier received in the digital certificate to determine a first match result;

a second comparator that compares the decrypted first contextual attributes to reference attributes, which are known to the host, to determine a second match result; and

a validating component that validates a portion of the digital certificate if the first and second match results both indicate a match.

46. (New) The host of claim 45, further comprising:

a combiner that combines the encrypted first contextual attributes, the encrypted unique device identifier, and the unique device identifier to produce a message authentication code (MAC);

an encrypting component that encrypts the MAC to generate an encrypted MAC; and

a third comparator that compares the generated encrypted MAC with an encrypted MAC received in the digital certificate to produce a third match result, wherein

the validating component validates the digital certificate if the first, second, and third match results all indicate a match.

47. (New) The host of claim 45, wherein:

the unique device identifier is decrypted with an asymmetric decryption key; and

the first contextual attributes are decrypted with a symmetric decryption key.

48. (New) The host of claim 46, wherein:

the unique device identifier is decrypted with an asymmetric decryption key;

the first contextual attributes are decrypted with a symmetric decryption key; and

the MAC is encrypted with a symmetric encryption key.

49. (New) The host of claim 46, wherein the combiner combines second contextual attributes of the PSD, which are received in the digital certificate, with the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes to produce the MAC.

50. (New) A method of generating a digital certificate within a personal security device (PSD), the method comprising:

encrypting a unique device identifier for the PSD to produce an encrypted unique device identifier;

encrypting first contextual attributes of the PSD to produce encrypted first contextual attributes;

combining the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes to generate the digital certificate, wherein

the unique device identifier and first contextual attributes are encrypted using different encryption keys.

51. (New) The method of claim 50, further comprising:

encrypting the combined encrypted first contextual attributes, encrypted unique device identifier, and unique device identifier to produce an encrypted message authentication code (MAC); and

combining the encrypted MAC with the unique device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes in the digital certificate.

52. (New) The method of claim 50, wherein:

the unique device identifier is encrypted with an asymmetric encryption key; and

the first contextual attributes are encrypted with a symmetric encryption key.

53. (New) The method of claim 51, wherein:

the unique device identifier is encrypted with an asymmetric encryption key;

the first contextual attributes are encrypted with a first symmetric encryption key; and

the MAC is encrypted with a second symmetric encryption key.

54. (New) The method of claim 50, further comprising combining second contextual attributes of the PSD with the unique

device identifier, the encrypted unique device identifier, and the encrypted first contextual attributes in the digital certificate.

55. (New) The method of claim 54, further comprising:

encrypting the combined encrypted first contextual attributes, second contextual attributes, encrypted unique device identifier, and unique device identifier to produce an encrypted message authentication code (MAC); and

combining the encrypted MAC with the unique device identifier, the encrypted unique device identifier, the encrypted first contextual attributes, and the second contextual attributes in the digital certificate.

56. (New) The method of claim 55, wherein:

the unique device identifier is encrypted with an asymmetric encryption key;

the first contextual attributes are encrypted with a first symmetric encryption key; and

the MAC is encrypted with a second symmetric encryption key.

57. (New) A method of validating a digital certificate that is received from a personal security device (PSD), the method comprising:

decrypting an encrypted unique device identifier for the PSD, which is received in the digital certificate, to produce a decrypted unique device identifier;

decrypting encrypted first contextual attributes of the PSD, which are received in the digital certificate, to produce decrypted first contextual attributes;

comparing the decrypted unique device identifier to a unique device identifier received in the digital certificate to determine a first match result;

comparing the decrypted first contextual attributes to reference attributes to determine a second match result; and

validating a portion of the digital certificate if the first and second match results both indicate a match.

58. (New) The method of claim 57, further comprising:

combining the encrypted first contextual attributes, the encrypted unique device identifier, and the unique device identifier to produce a message authentication code (MAC);

encrypting the MAC to generate an encrypted MAC;

comparing the generated encrypted MAC with an encrypted MAC received in the digital certificate to produce a third match result; and

validating the digital certificate if the first, second, and third match results all indicate a match.

59. (New) The method of claim 57, wherein:

the unique device identifier is decrypted with an asymmetric decryption key; and

the first contextual attributes are decrypted with a symmetric decryption key.

60. (New) The method of claim 58, wherein:

the unique device identifier is decrypted with an asymmetric decryption key;

the first contextual attributes are decrypted with a symmetric decryption key; and

the MAC is encrypted with a symmetric encryption key.

61. (New) The method of claim 58, further comprising combining second contextual attributes of the PSD, which are received in the digital certificate, with the unique device

identifier, the encrypted unique device identifier, and the encrypted first contextual attributes to produce the MAC.